دليل إدارة الكمبيوتر المكتبي

أجهزة الكمبيوتر المكتبية للأعمال

Document Part Number: 312947-172

سبتمبر ٢٠٠٣

يوفر هذا الدليل تعريفات وإرشادات تتعلق باستخدام ميزات الحماية وIntelligent Manageability المثبتة مسبقاً على طرازات مختارة.

إن Hewlett-Packard Company غير مسؤولة عن الأخطاء التقنية أو التحريرية أو النواقص التي يحويها هذا الدليل أو عن الأضرار العرضية أو الناتجة والمتعلقة بالتزويد بهذه المواد، أو أدائها، أو استخدامها. إن المعلومات الموجودة في هذا المستند معطاة "كما هي" دون كفالة من أي نوع، بما في ذلك ودون حصر، الكفالات الضمنية المتعلقة بإمكانية التسويق والملاءمة لغرض معيّن، وهي عرضة للتغيير دون سابق إشعار. إن الكفالات الخاصة بمنتجات HP محددة في النصوص الواضحة للكفالة المحدودة التي تصحب مثل هذه المنتجات. يجب عدم اعتبار أي مما ورد هنا على أنه عبارة عن كفالة إضافية.

تحذير: يشير النص الوارد على هذا النحو إلى أن عدم اتباع الإرشادات قد يؤدي إلى الإصابات الجسدية أو مفارقة الحياة.

إنذار: يشير النص الوارد على هذا النحو إلى أن عدم اتباع الإرشادات قد يؤدي إلى إلحاق الضرر بالأجهزة أو فقدان المعلومات.

دليل إدارة الكمبيوتر المكتبي

أجهزة الكمبيوتر المكتبية للأعمال

الطبعة الثانية (سبتمبر ٢٠٠٣)
Document Part Number: 312947-172

المحتويات

دليل إدارة الكمبيوتر المكتبي

التكوين والنشر الأولي ٢
تثبيت النظام عن بعد (Remote System Installation) ٣
تحديث البرامج وإدارتها ٤
البرنامج HP Client Manager ٤
Altiris Solutions ٤
Altiris PC Transplant Pro ٥
System Software Manager ٦
Proactive Change Notification ٦
ActiveUpdate ٦
ROM Flash ٧
Remote ROM Flash ٧
HPQFlash ٨
FailSafe Boot Block ROM ٨
تكرار نسخة متطابقة عن الإعداد ١٠
زر التشغيل ثنائي الحالة ١٩
موقع World Wide Web ٢٠
التجمعات والشركاء ٢٠
تعقب الموجودات وحمايتها ٢١
الحماية بواسطة كلمة مرور ٢٥
إنشاء كلمة مرور الإعداد باستخدام Computer Setup ٢٥
إنشاء كلمة مرور بدء التشغيل باستخدام Computer Setup ٢٦
الحماية المضمّنة ٣٠
DriveLock ٣٩
متحسّس الغطاء Smart Cover Sensor ٤١
Smart Cover Lock ٤٢
حماية سجل التمهيد الرئيسي Master Boot Record Security ٤٥
قبل تجزئة القرص الحالي القابل للتمهيد أو تهيئته ٤٧
قفل الكبل ٤٧
تقنية التعرّف على بصمات الأصابع Fingerprint Identification Technology ٤٨

الإعلام عن الخطأ والاستعادة Fault Notification and Recovery ٤٨
نظام حماية محركات الأقراص Drive Protection System ٤٨
وحدة تزويد بالطاقة تحتمل التغيّر المفاجئ في الفولتية ٤٩
المتحسس الحراري ٤٩

الفهرس

دليل إدارة الكمبيوتر المكتبي

توفر HP Intelligent Manageability حلولاً قياسية لإدارة أجهزة الكمبيوتر الشخصية المكتبية، ومحطات العمل، والأجهزة المحمولة، والتحكم بها في بيئة شبكة الاتصال. وقد مهّدت HP الطريق لإدارة الكمبيوتر المكتبي عام ١٩٩٥ مع إطلاقها المجموعة الأولى من أجهزة الكمبيوتر الشخصية المكتبية القابلة للإدارة بشكل كامل. وتحتفظ HP ببراءة اختراع في مجال تكنولوجيا الإدارة. ومنذ ذلك الوقت، قادت شركة HP مجهوداً واسعاً في مجال الصناعة من أجل تطوير المقاييس والبنية التحتية المطلوبة لنشر، وتكوين، وإدارة أجهزة الكمبيوتر الشخصية المكتبية، ومحطات العمل، والأجهزة المحمولة. وتعمل شركة HP عن كثب مع موفري حلول برامج الإدارة الرواد في الصناعة لضمان التوافق ما بين Intelligent Manageability وهذه المنتجات. ويمكن اعتبار Intelligent Manageability وجهاً هاماً لالتزامنا الشامل بتوفير الحلول لمساعدتك خلال المراحل الأربع من حياة أجهزة الكمبيوتر الشخصية المكتبية وهي التخطيط، والنشر، والإدارة، والمراحل الانتقالية.

القدرات والميزات الرئيسية لإدارة الكمبيوتر المكتبي هي:

- التكوين والنشر الأولي
- تثبيت النظام عن بعد
- تحديث البرامج وإدارتها
- إعادة برمجة ذاكرة ROM
- تعقب الموجودات وحمايتها
- الإعلام بالخطأ والاستعادة

قد يختلف الدعم المتوفر لميزات معيّنة يتم وصفها في هذا الدليل وذلك وفقاً للطراز أو لإصدار البرنامج.

التكوين والنشر الأولي

تجد في جهاز الكمبيوتر صورة مثبتة مسبقاً لبرامج النظام. وبعد عملية وجيزة من أجل "فك حزمة" البرامج، يصبح جهاز الكمبيوتر جاهزاً للاستخدام.

وقد تفضل استبدال الصورة المثبتة مسبقاً للبرامج بمجموعة مخصصة من برامج النظام والتطبيقات. هناك عدة أساليب لنشر صورة برامج مخصصة. وهي تتضمّن:

- تثبيت تطبيقات إضافية بعد فك حزمة البرامج المثبتة مسبقاً.
- استخدام أدوات نشر البرامج مثل Altiris Deployment Solution™ لاستبدال البرامج المثبتة مسبقاً بصورة برامج مخصصة.
- استخدام عملية استنساخ القرص لنسخ المحتويات من قرص ثابت إلى قرص ثابت آخر.

يتوقف أفضل أسلوب للنشر على بيئة تقنية المعلومات وطرق معالجتها المتوفرة لديك. ويوفر القسم PC Deployment في موقع HP Lifecycle Solutions على ويب (http://h18000.www1.hp.com/solutions/pcsolutions) معلومات تهدف إلى مساعدتك على اختيار الأسلوب الأفضل للنشر.

يوفر القرص المضغوط *Restore Plus!*، والإعداد المستند إلى ROM، وأجهزة ACPI، مساعدة إضافية في مجال استعادة برامج النظام، وإدارة التكوين واستكشاف أخطائه وإصلاحها، وإدارة الطاقة.

تثبيت النظام عن بعد (Remote System Installation)

تسمح لك ميزة Remote System Installation ببدء تشغيل النظام وإعداده باستخدام المعلومات حول البرامج والتكوين الموجودة على ملقم شبكة الاتصال وذلك ببدء Preboot Execution Environment (PXE). وتُستخدم ميزة Remote System Installation عادة كأداة لإعداد النظام وتكوينه، ويمكنك استخدامها لتنفيذ المهام التالية:

- تهيئة محرك قرص ثابت.
- نشر صورة برنامج على جهاز واحد أو أكثر من أجهزة الكمبيوتر الشخصية الجديدة.
- تحديث BIOS النظام عن بعد في flash ROM (Remote ROM Flash على الصفحة ٧)
- تكوين إعدادات BIOS للنظام

لبدء Remote System Installation، اضغط **F12** عندما تظهر رسالة F12=Network Service Boot في الزاوية اليمنى السفلى لشاشة شعار HP. اتبع الإرشادات التي تظهر على الشاشة لمتابعة تنفيذ العملية. ترتيب التمهيد الافتراضي هو إعداد تكوين BIOS يمكن تغييره من أجل المحاولة دائماً لتمهيد PXE.

لقد اشتركت HP و Altiris, Inc. لتوفير الأدوات المصممة لجعل مهمة إدارة ونشر البرامج على أجهزة الكمبيوتر الشخصي في الشركات أكثر سهولة وأقل استهلاكاً للوقت، مما يؤدي إلى تخفيض الكلفة الكلية للملكية وجعل أجهزة HP أكثر أجهزة الكمبيوتر الشخصية قابلية للإدارة في بيئة الشركات.

تحديث البرامج وإدارتها

توفر HP العديد من الأدوات لإدارة البرامج وتحديثها على أجهزة الكمبيوتر المكتبية ومحطات العمل — Altiris؛ و Altiris PC Transplant Pro؛ و HP Client Manager Software، حل Altiris؛ و System Software Manager؛ و Proactive Change Notification؛ و Active Update.

البرنامج HP Client Manager

يتكامل البرنامج Intelligent HP Client Manager Software (HP CMS) إلى حد بعيد مع تقنية HP Intelligent Manageability ضمن Altiris لتوفير إمكانيات أكبر لإدارة الأجهزة التي تتصل بها أجهزة HP بما فيها:

- تقارير مفصلة حول الأجهزة المتوفرة وذلك من أجل إدارة الموجودات
- المراقبة التفقدية لسلامة الكمبيوتر الشخصي والتشخيص
- الإشعار المسبق حول التغييرات في بيئة الأجهزة
- رفع التقارير التي يمكن الوصول إليها على ويب للإعلام عن تفاصيل تؤثر بشكل كبير على سير الأعمال كالآلات التي تصدر عنها تحذيرات متعلقة بالحرارة، وإنذارات حول الذاكرة، وغيرها
- التحديث عن بعد لبرامج النظام كبرامج التشغيل وذاكرة ROM BIOS
- تغيير عن بعد لترتيب التمهيد

للحصول على مزيد من المعلومات حول HP Client Manager، تفضّل بزيارة الموقع http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

توفر HP Client Management Solutions إدارة مركزية للأجهزة لأجهزة عملاء HP تتعلق بكافة نواحي التطورات التي تمر بها تكنولوجيا المعلومات.

- إدارة قوائم الجرد والموجودات
  - ❑ الالتزام بترخيص البرامج
  - ❑ تعقّب أجهزة الكمبيوتر والإعلام عنها
  - ❑ عقد الاستئجار، وتعقّب الموجودات الثابتة

- النشر والترحيل
  - ترحيل Microsoft Windows 2000 أو Windows XP Professional أو Home Edition
  - نشر النظام
  - ترحيل الإعدادات الشخصية
- مكتب المساعدة وحل المشاكل
  - إدارة تذاكر مكتب المساعدة
  - استكشاف الأخطاء عن بعد وإصلاحها
  - حل المشاكل عن بعد
  - الاسترداد من الحالات غير القابلة للإصلاح
- إدارة البرامج والعمليات
  - إدارة الكمبيوتر المكتبي
  - نشر برامج نظام HP
  - الإصلاح الذاتي للتطبيقات

في بعض طرازات مختارة من أجهزة الكمبيوتر المكتبية وأجهزة الكمبيوتر المحمول، يتم تضمين عامل إدارة Altiris كجزء من نسخة البرنامج المحمّلة من قبل الشركة المصنّعة. ويمكّن هذا العامل التواصل مع Altiris Development Solution، الذي يمكن استخدامه لإتمام عملية نشر على الأجهزة الجديدة أو ترحيل الإعدادات الشخصية إلى نظام تشغيل جديد باستخدام معالجات يسهل تتبّعها. وتوفر حلول Altiris قدرات توزيع برامج سهلة الاستخدام. وعند استخدامه بالتزامن مع System Software Manager أو HP Client Manager، سيكون باستطاعة المسؤولين أيضاً تحديث ROM BIOS وبرامج تشغيل الأجهزة من وحدة تحكم مركزية.

للحصول على مزيد من المعلومات، يمكنك زيارة موقع HP على ويب على العنوان: http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

تسمح لك الأداة Altiris PC Transplant Pro بترحيل الكمبيوتر الشخصي دون عناء بالحفاظ على الإعدادات القديمة، والتفضيلات، والبيانات وترحيلها إلى البيئة الجديدة بسرعة وسهولة. وهكذا تستغرق عمليات الترقية دقائق عوضاً عن ساعات أو أيام، ويبدو سطح المكتب ويعمل تماماً كما يتوقع المستخدمون.

للحصول على مزيد من المعلومات والتفاصيل حول كيفية تحميل إصدار تقييمي صالح لمدة ٣٠ يوماً ويتضمن الوظائف كاملة، تفضّل بزيارة الموقع http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

تسمح لك الأداة المساعدة System Software Manager (SSM) بتحديث برامج على مستوى النظام على أجهزة كمبيوتر متعددة في الوقت نفسه. وعند تشغيلها على نظام كمبيوتر عميل، تكشف SSM إصدارات الأجهزة والبرامج، ثم تحدّث البرامج المناسبة من خلال المخزن المركزي، والذي يُعرَف أيضاً بمخزن الملفات. ويشار إلى إصدارات برامج التشغيل Drivers التي تعتمدها الأداة SSM بواسطة رمز خاص في موقع ويب المعني بتحميل برامج التشغيل وفي القرص المضغوط Support Software. لتحميل الأداة المساعدة أو للحصول على مزيد من المعلومات حول SSM، تفضّل بزيارة الموقع http://h18000.www1.hp.com/im/ssmwp.html.

Proactive Change Notification

يستخدم البرنامج Proactive Change Notification موقع ويب Subscriber's Choice من أجل القيام بشكل تلقائي ومبكر بما يلي:

- إرسال رسائل بريد إلكتروني خاصة بـــ Proactive Change Notification (PCN) لإعلامك بالتغييرات في الأجهزة والبرامج المتعلقة بمعظم أجهزة الكمبيوتر والملقمات المباعة في الأسواق، قبل ٦٠ يوماً على الأقل من حدوثها.
- إرسال رسائل بريد إلكتروني تتضمن Customer Bulletins، Customer Advisories، وCustomer Notes، وSecurity Bulletins، وDriver alerts تتعلق بمعظم أجهزة الكمبيوتر والملقمات المباعة في الأسواق.

ويمكنك إنشاء ملف تعريف خاص بك للتأكد من تلقيك فقط المعلومات المتعلقة ببيئة تكنولوجيا معلومات معيّنة. ولمعرفة المزيد عن برنامج Proactive Change Notification وإنشاء ملف تعريف مخصص، تفضّل بزيارة الموقع http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate هو عبارة عن تطبيق من HP يستند إلى العملاء. ويتم تشغيل عميل ActiveUpdate على النظام المحلي ويستخدم ملف التعريف المعرّف من قبل المستخدم والخاص بك من أجل تحميل تحديثات البرامج تلقائياً وذلك في معظم أجهزة الكمبيوتر والملقمات من HP المباعة في الأسواق. تحديثات البرامج المحمّلة هذه يمكن أن يتم نشرها بطريقة ذكية إلى الأجهزة المخصصة لها من قبل HP Client Manager Software وSystem Software Manager.

لمعرفة المزيد حول ActiveUpdate، وتحميل التطبيق، وإنشاء ملف تعريف مخصص، تفضّل بزيارة الموقع http://h18000.www1.hp.com/products/servers/management/active update/index.html.

ROM Flash

يتضمّن الكمبيوتر ذاكرة flash ROM قابلة لإعادة البرمجة (ذاكرة القراءة فقط) قابلة لإعادة البرمجة. ويمكنك حماية ذاكرة ROM من التعرّض للتحديث أو الكتابة فوقها بطريق الخطأ، من خلال إنشاء كلمة مرور الإعداد في الأداة المساعدة لإعداد الكمبيوتر Computer Setup (**F10**). ويعتبر هذا الأمر هاماً لضمان تشغيل الكمبيوتر بشكل سليم وموثوق. وإذا احتجت إلى ترقية ROM أو أردت ترقيتها، فيمكنك:

- طلب إصدار ترقية للقرص المرن *ROMPaq* من HP.
- تحميل أحدث نسخة من صور برامج ROMPaq من الموقع http://h18000.www1.hp.com/im/ssmwp.html.

إنذار: لتوفير أقصى درجات الحماية لـــ ROM، تأكد من إنشاء كلمة مرور الإعداد. فكلمة المرور هذه تمنع عمليات ترقية ROM غير المسموح بها. ويسمح System Software Manager للمسؤول عن النظام بتعيين كلمة مرور الإعداد على جهاز كمبيوتر شخصي واحد أو أكثر في الوقت نفسه. للحصول على مزيد من المعلومات، تفضّل بزيارة الموقع http://h18000.www1.hp.com/im/ssmwp.html.

Remote ROM Flash

يسمح Remote ROM Flash للمسؤول عن النظام بترقية ROM بطريقة آمنة على أجهزة كمبيوتر HP البعيدة، مباشرة من وحدة تحكم إدارة شبكة الاتصال المركزية. يؤدي تمكين المسؤول عن النظام من تنفيذ هذه المهمة عن بعد وعلى أجهزة كمبيوتر متعددة، إلى النشر المتناسق لصور ROM على أجهزة كمبيوتر HP وزيادة التحكم بها عبر شبكة الاتصال. كما ينتج عن ذلك إنتاجية أكبر وانخفاض في التكاليف الإجمالية للملكية.

يجب أن يكون الكمبيوتر قيد التشغيل أو يجب تشغيله عن بعد باستخدام Remote Wakeup للاستفادة من Remote ROM Flash.

للحصول على مزيد من المعلومات حول Remote ROM Flash، يمكنك الرجوع إلى HP Client Manager أو System Software Manager على العنوان http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

تُستخدم الأداة المساعدة HPQFlash لتحديث System ROM محلياً أو استعادتها على أجهزة كمبيوتر فردية من خلال نظام التشغيل Windows.

للحصول على مزيد من المعلومات حول HPQFlash، تفضّل بزيارة الموقع http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

FailSafe Boot Block ROM

تسمح FailSafe Boot Block ROM باستعادة النظام في حال حدوث عطل أثناء إعادة برمجة ROM، على سبيل المثال عند انقطاع التيار الكهربائي أثناء ترقية ROM. ويعتبر Boot Block بمثابة قسم محمي من التفريغ في ROM يبحث عن تحديث صالح لذاكرة ROM النظام عند تشغيل الكمبيوتر بإمداده بالطاقة.

- إذا كانت ذاكرة ROM النظام صالحة، يبدأ تشغيل النظام بشكل طبيعي.
- إذا لم تكن ذاكرة ROM النظام صالحة، فإن FailSafe Boot Block ROM يوفر دعماً كافياً لبدء تشغيل النظام من القرص المرن لـــ ROMPaq، الذي يبرمج ذاكرة ROM النظام باستخدام صورة صالحة.

عندما يكشف Boot Block عن ذاكرة ROM نظام غير صالحة، تومض أضواء System Power LED باللون الأحمر ٨ مرات، مرة كل ثانية، تليها فترة توقف مؤقت من ثانيتين. كما ستسمع ٨ أصوات تنبيه متزامنة. وتظهر على الشاشة (في بعض الطرازات) رسالة إعلام بوضع استعادة Boot Block.

لاستعادة النظام بعد دخوله في وضع استعادة Boot Block، أكمل الخطوات التالية:

١. أخرج القرص المرن من محركه، في حال وجوده فيه، وأوقف تشغيل الكمبيوتر.
٢. أدخل القرص المرن ROMPaq في محرك الأقراص المرنة.
٣. شغّل الكمبيوتر.
٤. إذا تعذّر العثور على القرص المرن ROMPaq، فستتم مطالبتك بإدخال القرص وإعادة تشغيل الكمبيوتر.
٥. إذا كان قد تم إنشاء كلمة مرور الإعداد، فيبدأ تشغيل ضوء Caps Lock وتتم مطالبتك بإدخال كلمة المرور.

٦. أدخل كلمة مرور الإعداد.

٧. إذا نجحت عملية بدء تشغيل النظام من القرص المرن وأعاد النظام برمجة ROM بنجاح، فسيتم تشغيل الأضواء الثلاثة للوحة المفاتيح. كما تشير سلسلة من أصوات التنبيه المتعالية إلى إتمام العملية بنجاح.

٨. أخرج القرص المرن وافصل الطاقة.

٩. شغّل الطاقة مرة أخرى لإعادة تشغيل الكمبيوتر.

يسرد الجدول التالي التركيبات المختلفة لأضواء لوحة المفاتيح المستخدمة من قبل Boot Block ROM، (عندما تكون لوحة مفاتيح PS/2 موصولة بالكمبيوتر)، كما يفسر معنى كل تركيب والإجراء المقترن به.

تركيبات أضواء لوحة المفاتيح المستخدمة من قبل Boot Block ROM

وضع FailSafe Boot Block	لون ضوء لوحة المفاتيح	نشاط ضوء لوحة المفاتيح	الحالة/الرسالة
Num Lock	أخضر	تشغيل	القرص المرن RomPaq غير موجود، أو غير صالح، أو أن محرك الأقراص غير جاهز.*
Caps Lock	أخضر	تشغيل	أدخل كلمة المرور.*
Num, Caps, Scroll Lock	أخضر	تشغيل وإيقاف تشغيل مرتين (يرافق ذلك صوت تنبيه طويل وثلاثة أصوات تنبيه قصيرة)	فشل في إعادة برمجة ROM.*
Num, Caps, Scroll Lock	أخضر	تشغيل	نجاح Boot Block ROM Flash. يجب إيقاف التشغيل، ثم إعادة التشغيل من أجل التمهيد.

✎ لا تومض أضواء التشخيص على لوحات مفاتيح USB.

تكرار نسخة متطابقة عن الإعداد

توفر الإجراءات التالية للمسؤول القدرة على نسخ تكوين الإعداد من كمبيوتر ما إلى أجهزة كمبيوتر أخرى من الطراز نفسه وبسهولة. وهذا ما يسمح بتكوين أجهزة كمبيوتر متعددة بشكل أسرع وأكثر تناسقا.

يتطلب الإجراءان محرك أقراص مرنة أو جهاز USB flash media معتمدا، مثل HP Drive Key.

النسخ إلى كمبيوتر واحد

إنذار: تكوين الإعداد يعتبر خاصا بطراز الكمبيوتر. فإذا لم يكن الكمبيوتر المصدر والكمبيوتر الهدف من الطراز نفسه، فقد ينتج عن ذلك تلف نظام الملفات. فعليك مثلا ألا تنسخ تكوين الإعداد من D510 Ultra-slim Desktop إلى D510 e-pc.

١. حدد تكوين إعداد تريد نسخه. شغل الكمبيوتر أو أعد تشغيله. إذا كنت تعمل ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

٣. أدخل قرصا مرنا أو جهاز USB flash media.

٤. انقر فوق **File > Save to Diskette**. اتبع الإرشادات التي تظهر على الشاشة لإنشاء قرص مرن للتكوين أو جهاز USB flash media.

٥. أوقف تشغيل الكمبيوتر المحمول الذي تريد تكوينه وأدخل القرص المرن للتكوين أو جهاز USB flash media.

٦. شغل الكمبيوتر المحمول الذي تريد تكوينه. اضغط المفتاح F10 عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

٧. انقر فوق **File > Restore from Diskette**، واتبع الإرشادات التي تظهر على الشاشة.

٨. أعد تشغيل الكمبيوتر المحمول عند اكتمال التكوين.

إنذار: تكوين الإعداد يعتبر خاصا بطراز الكمبيوتر. فإذا لم يكن الكمبيوتر المصدر والكمبيوتر الهدف من الطراز نفسه، فقد ينتج عن ذلك تلف نظام الملفات. فعليك مثلا ألا تنسخ تكوين الإعداد من D510 Ultra-slim Desktop إلى D510 e-pc.

هذا الأسلوب يستغرق وقتا أطول بقليل لتكوين القرص المرن للتكوين أو جهاز USB flash media، غير أن نسخ التكوين إلى أجهزة الكمبيوتر الهدف هو أسرع إلى حد بعيد.

لا يمكن إنشاء قرص مرن قابل للتمهيد في Windows 2000. القرص المرن القابل للتمهيد مطلوب لتنفيذ هذا الإجراء أو لإنشاء جهاز USB flash media قابل للتمهيد. إذا لم يكن Windows 9x أو Windows XP متوفرا للاستخدام من أجل إنشاء قرص مرن قابل للتمهيد، فاستخدم أسلوب النسخ إلى كمبيوتر واحد عوضا عن ذلك (انظر "النسخ إلى كمبيوتر واحد" على الصفحة ١٠).

١. أنشئ قرصا مرنا قابلا للتمهيد أو جهاز USB flash media. انظر "القرص المرن القابل للتمهيد" على الصفحة ١٢، أو "جهاز USB Flash Media المعتمد القابل للتمهيد على الصفحة ١٣" أو "جهاز USB Flash Media غير المعتمد القابل للتمهيد" على الصفحة ١٦.

إنذار: لا يمكن أن يتم تمهيد كافة أجهزة الكمبيوتر من جهاز USB flash media. إذا ذكر ترتيب التمهيد الافتراضي في Computer Setup (F10) Utility جهاز USB قبل محرك القرص الثابت، فيمكن تمهيد الكمبيوتر من جهاز USB flash media. وإلا، فيجب استخدام قرص مرن قابل للتمهيد.

٢. حدد تكوين إعداد تريد نسخه. شغل الكمبيوتر أو أعد تشغيله. إذا كنت تعمل ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٣. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

٤. أدخل القرص المرن القابل للتمهيد أو جهاز USB flash media.

٥. انقر فوق **File > Save to Diskette**. اتبع الإرشادات التي تظهر على الشاشة لإنشاء القرص المرن للتكوين أو جهاز USB flash media.

٦. قم بتحميل أداة BIOS مساعدة لإجراء نسخ متطابق للإعداد (repset.exe) وانسخها إلى القرص المرن للتكوين أو جهاز USB flash media. هذه الأداة المساعدة موجودة في الموقع http://h18000.www1.hp.com/support/files/hpcpqdt/us/downlo ad/18040.html.

٧. على القرص المرن للتكوين أو جهاز USB flash media، أنشئ ملف autoexec.bat يحتوي على الأمر التالي:

repset.exe

٨. أوقف تشغيل الكمبيوتر المحمول الذي تريد تكوينه. أدخل القرص المرن للتكوين أو جهاز USB flash media وشغل الكمبيوتر. فيتم تشغيل الأداة المساعدة للإعداد تلقائيا.

٩. أعد تشغيل الكمبيوتر عند اكتمال التكوين.

إنشاء جهاز قابل للتمهيد

القرص المرن القابل للتمهيد

هذه الإرشادات تتعلق بـــ Windows XP Professional و Home Edition. ولا يعتمد Windows 2000 إنشاء الأقراص المرنة القابلة للتمهيد.

١. أدخل قرصا مرنا في محرك الأقراص المرنة.

٢. انقر فوق **Start**، ثم فوق **My Computer**.

٣. انقر بزر الماوس الأيمن فوق محرك الأقراص المرنة، ثم انقر فوق **Format**.

٤. حدد خانة الاختيار **Create an MS-DOS startup disk**، ثم انقر فوق **Start**.

عد إلى "النسخ إلى أجهزة كمبيوتر متعددة" على الصفحة ١١.

جهاز USB Flash Media المعتمد

تتوفر في أجهزة معتمدة، مثل HP Drive Key أو DiskOnKey، نسخة مثبّتة مسبقاً بهدف تبسيط عملية جعل هذه الأجهزة قابلة للتمهيد. وإذا لم تتوفر هذه النسخة لـــ Drive Key الذي يتم استخدامه، فاستخدم الإجراء لاحقاً في هذا الفصل. (انظر "جهاز USB Flash Media غير المعتمد القابل للتمهيد" على الصفحة ١٦).

إنذار: لا يمكن أن يتم تمهيد كافة أجهزة الكمبيوتر من جهاز USB flash media. إذا ذكر ترتيب التمهيد الافتراضي في Computer Setup (F10) Utility جهاز USB قبل محرك القرص الثابت، فيمكن تمهيد الكمبيوتر من جهاز USB flash media. وإلا، فيجب استخدام قرص مرن قابل للتمهيد.

لإنشاء جهاز USB flash media قابل للتمهيد، يجب أن يتوفر لديك:

- أحد أنظمة التشغيل التالية:
  - ❑ Compaq Evo D510 Ultra-slim Desktop
  - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor
  - ❑ HP Compaq Business Desktop d530 Series - Ultra-slim Desktop، أو Small Form Factor، أو Convertible Minitower
  - ❑ أجهزة الكمبيوتر المحمول Compaq Evo N400c، أو N410c، أو N600c، أو N610c، أو N620c، أو N800c، أو N1000c
  - ❑ أجهزة الكمبيوتر المحمول Compaq Presario 1500 أو ٢٨٠٠

  ووفقا لـــ BIOS الفردي، فقد تعتمد الأنظمة المستقبلية أيضا التمهيد إلى HP Drive Key.

إنذار: إذا كنت تستخدم جهاز كمبيوتر آخر غير الجهاز المذكور أعلاه، فتأكد من أن ترتيب التمهيد الافتراضي في Computer Setup (F10) Utility يذكر جهاز USB قبل محرك القرص الثابت.

- إحدى وحدات التخزين التالية:
  - ❑ 16MB HP Drive Key
  - ❑ 32MB HP Drive Key
  - ❑ 32MB DiskOnKey
  - ❑ 64MB HP Drive Key
  - ❑ 64MB DiskOnKey

- ❑ 128MB HP Drive Key
- ❑ 128MB DiskOnKey

■ قرص DOS مرن قابل للتمهيد مع البرنامجين FDISK وSYS. إذا لم يكن SYS متوفراً، فيمكنك استخدام FORMAT، غير أنه سيتم فقدان كافة الملفات الموجودة على Drive Key.

١. أوقف تشغيل الكمبيوتر.

٢. أدخل Drive Key في أحد منافذ USB للكمبيوتر وأخرج كافة أجهزة USB الأخرى للتخزين باستثناء محركات أقراص USB المرنة.

٣. أدخل قرص DOS مرن قابل للتمهيد يتضمّن FDISK.COM وإما SYS.COM أو FORMAT.COM في محرك أقراص مرنة وشغّل الكمبيوتر للتمهيد إلى قرص DOS المرن.

٤. شغّل FDISK من الموجّه A:\ وذلك بكتابة **FDISK** وضغط Enter. انقر فوق Yes (Y) عند المطالبة وذلك لتمكين اعتماد القرص الكبير الحجم.

٥. أدخل الخيار [**5**] لعرض محركات الأقراص الموجودة في النظام. وسيكون Drive Key محرك الأقراص الأقرب من حيث الحجم إلى أحد محركات الأقراص المذكورة. وهو عادة محرك الأقراص الأخير في القائمة. سجّل حرف محرك الأقراص.

محرك أقراص Drive Key: _____

إنذار: إذا لم يتطابق أحد محركات الأقراص مع Drive Key، فلا تباشر بالتنفيذ. فقد يحدث فقدان للبيانات. دقق في كافة منافذ USB للعثور على أجهزة تخزين إضافية. إذا تم العثور على أي جهاز تخزين، فعليك إخراجه، وإعادة تمهيد الكمبيوتر، ومتابعة التنفيذ من الخطوة ٤. وإذا لم يتم العثور على أي جهاز تخزين، فهذا يعني أن النظام لا يعتمد Drive Key أو أن Drive Key فيه خلل ما. لا تباشر في عملية جعل Drive Key قابلاً للتمهيد.

٦. قم بإنهاء FDISK بضغط المفتاح **Esc** للعودة إلى الموجّه A:\.

٧. إذا احتوى قرص DOS المرن القابل للتمهيد على SYS.COM، فانتقل إلى الخطوة ٨، وإلا فانتقل إلى الخطوة ٩.

٨. عند الموجّه A:\، أدخل **SYS x:** حيث يمثّل x حرف محرك الأقراص المسجّل أعلاه. انتقل إلى الخطوة ١٣.

إنذار: تأكد من إدخال الحرف الصحيح لمحرك الأقراص الخاص بـــ Drive Key.

بعد أن يتم نقل ملفات النظام، سيعود SYS إلى الموجه A:\.

٩. انسخ أية ملفات تريد أن تحتفظ بها من Drive Key إلى دليل مؤقت على محرك أقراص آخر (مثلا، محرك الأقراص الثابت الداخلي للنظام).

١٠. عند الموجه A:\، أدخل **FORMAT /S X:** حيث يمثل X حرف محرك الأقراص المسجل أعلاه.

إنذار: تأكد من إدخال الحرف الصحيح لمحرك الأقراص الخاص بـــ Drive Key.

سيعرض FORMAT تحذيرا واحدا أو أكثر وفي كل مرة سيسألك فيها عما إذا كنت تريد المتابعة. أدخل **y** في كل مرة. وسيقوم FORMAT بتهيئة Drive Key، وإضافة ملفات النظام، ويسألك عن تسمية وحدة التخزين.

١١. اضغط **Enter** في حال عدم وجود تسمية أو أدخل تسمية إن أردت ذلك.

١٢. انسخ أية ملفات قمت بحفظها في الخطوة ٩ لإعادتها إلى Drive Key.

١٣. أخرج القرص المرن وأعد تمهيد الكمبيوتر. وسيتم تمهيد الكمبيوتر إلى Drive Key كمحرك الأقراص C.

يختلف ترتيب التمهيد الافتراضي من كمبيوتر إلى آخر، ويمكن تغييره في Computer Setup (F10) Utility.

إذا كنت قد استخدمت إصدار DOS من Windows 9x، فقد تشاهد شاشة شعار Windows مختصرة. إذا لم ترغب في ظهور هذه الشاشة، أضف ملفا مسمى LOGO.SYS بطول صفر إلى الدليل الجذر لـــ Drive Key.

عد إلى "النسخ إلى أجهزة كمبيوتر متعددة" على الصفحة ١١.

جهاز USB Flash Media غير المعتمد

إنذار: لا يمكن أن يتم تمهيد كافة أجهزة الكمبيوتر من جهاز USB flash media. إذا ذكر ترتيب التمهيد الافتراضي في Computer Setup (F10) Utility جهاز USB قبل محرك القرص الثابت، فيمكن تمهيد الكمبيوتر من جهاز USB flash media. وإلا، فيجب استخدام قرص مرن قابل للتمهيد.

لإنشاء جهاز USB flash media قابل للتمهيد، يجب أن يتوفر لديك:

- أحد أنظمة التشغيل التالية:
  - ❑ Compaq Evo D510 Ultra-slim Desktop
  - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor
  - ❑ HP Compaq Business Desktop d530 Series - Ultra-slim Desktop، أو Small Form Factor، أو Convertible Minitower
  - ❑ أجهزة الكمبيوتر المحمول Compaq Evo N400c، أو N410c، أو N600c، أو N610c، أو N620c، أو N800c، أو N1000c
  - ❑ أجهزة الكمبيوتر المحمول Compaq Presario 1500 أو ٢٨٠٠

ووفقا لـــ BIOS الفردي، فقد تعتمد الأنظمة المستقبلية أيضا التمهيد إلى USB flash media.

إنذار: إذا كنت تستخدم جهاز كمبيوتر آخر غير الجهاز المذكور أعلاه، فتأكد من أن ترتيب التمهيد الافتراضي في Computer Setup (F10) Utility يذكر جهاز USB قبل محرك القرص الثابت.

- قرص DOS مرن قابل للتمهيد مع البرنامجين FDISK وSYS. إذا لم يكن SYS متوفرا، فيمكنك استخدام FORMAT، غير أنه سيتم فقدان كافة الملفات الموجودة على Drive Key.

١. في حال وجود أية بطاقات PCI في النظام حيث تم توصيل محركات أقراص SCSI، أو ATA RAID، أو SATA، أوقف تشغيل الكمبيوتر وافصل سلك الطاقة.

إنذار: يجب أن يتم فصل سلك الطاقة.

٢. افتح الكمبيوتر وأخرج بطاقات PCI.

٣. أدخل جهاز USB flash media في أحد منافذ USB للكمبيوتر وأخرج كافة أجهزة USB الأخرى للتخزين باستثناء محركات أقراص USB المرنة. أغلق غطاء الكمبيوتر.

٤. وصل سلك الطاقة وشغل الكمبيوتر. عندما يتحول ضوء الشاشة إلى أخضر، اضغط المفتاح **F10** للانتقال إلى الأداة المساعدة لإعداد الكمبيوتر.

٥. انتقل إلى Advanced/PCI devices لتعطيل تشغيل جهازي تحكم IDE وSATA. وعند تعطيل جهاز التحكم SATA، سجل IRQ الذي تم تعيينه إلى جهاز التحكم. وستحتاج إلى إعادة تعيين IRQ في وقت لاحق. قم بإنهاء برنامج الإعداد، لتأكيد التغييرات.

SATA IRQ: _____

٦. أدخل قرص DOS مرن قابل للتمهيد يتضمن FDISK.COM وإما SYS.COM أو FORMAT.COM في محرك أقراص مرنة وشغل الكمبيوتر للتمهيد إلى قرص DOS المرن.

٧. شغل FDISK واحذف أية أقسام موجودة على جهاز USB flash media. أنشئ قسما جديدا وضع عليه علامة على أنه نشط. قم بإنهاء FDISK وذلك بضغط المفتاح **Esc**.

٨. إذا لم يتم تلقائيا إعادة تشغيل النظام عند إنهاء FDISK، فاضغط **Ctrl**+**Alt**+**Del** لإعادة التمهيد إلى قرص DOS المرن.

٩. عند موجه A:\، اكتب **FORMAT C: /S** واضغط **Enter**. وسيقوم Format بتهيئة جهاز USB flash media، وإضافة ملفات النظام، وطلب تسمية وحدة التخزين.

١٠. اضغط **Enter** في حال عدم وجود تسمية أو أدخل تسمية إن أردت ذلك.

١١. أوقف تشغيل الكمبيوتر وافصل سلك الطاقة. افتح الكمبيوتر وأعد تثبيت أية بطاقات PCI تم إخراجها في السابق. أغلق غطاء الكمبيوتر.

١٢. وصل سلك الطاقة، وأخرج القرص المرن، ثم شغل الكمبيوتر.

١٣. عندما يتحول ضوء الشاشة إلى أخضر، اضغط المفتاح **F10** للانتقال إلى الأداة المساعدة لإعداد الكمبيوتر.

١٤. انتقل إلى Advanced/PCI devices وأعد تمكين تشغيل جهازي تحكم IDE وSATA اللذين تم تعطيل تشغيلهما في الخطوة ٥. ضع جهاز تحكم SATA على IRQ الأصلي الخاص به.

١٥. احفظ التغييرات وقم بالإنهاء. سيتم تمهيد الكمبيوتر إلى جهاز USB flash media كمحرك أقراص C.

يختلف ترتيب التمهيد الافتراضي من كمبيوتر إلى آخر، ويمكن تغييره في Computer Setup (F10) Utility.

إذا كنت قد استخدمت إصدار DOS من Windows 9x، فقد تشاهد شاشة شعار Windows مختصرة. إذا لم ترغب في ظهور هذه الشاشة، أضف ملفا مسمى LOGO.SYS بطول صفر إلى الدليل الجذر لـــ Drive Key.

عد إلى "النسخ إلى أجهزة كمبيوتر متعددة" على الصفحة ١١.

زر التشغيل ثنائي الحالة

مع تمكين استخدام Advanced Configuration and Power Interface (ACPI) في Windows 2000، وWindows XP Professional وHome Edition، يمكن لزر التشغيل أن يعمل كمفتاح للتشغيل/إيقاف التشغيل أو كزر للتوقف المرحلي. ميزة التوقف المرحلي لا تقطع الطاقة تماما، بل تتسبب في دخول الكمبيوتر في وضع احتياطي يكون فيه استهلاك الطاقة منخفضا. وهذا ما يسمح لك بإيقاف التشغيل دون إغلاق التطبيقات والعودة بسرعة إلى حالة التشغيل نفسها دون فقدان البيانات.

لتغيير تكوين زر التشغيل، نفذ الخطوات التالية:

١. في Windows 2000، انقر بزر الماوس الأيسر فوق **الزر Start**، ثم حدد **Power Options < Control Panel < Settings**.

في Windows XP Professional وHome Edition، انقر بزر الماوس الأيسر فوق **الزر Start**، ثم حدد **Performance and < Control Panel Power Options < Maintenance**.

٢. في **Power Options Properties**، حدد علامة التبويب **Advanced**.

٣. في القسم **Power Button**، حدد الإعداد المطلوب لزر التشغيل.

بعد تكوين زر التشغيل بحيث يعمل كزر للتوقف المرحلي، اضغط هذا الزر لوضع النظام في حالة استهلاك للطاقة منخفض جدا (توقف مرحلي). اضغط الزر مرة أخرى لإخراج النظام بسرعة من حالة التوقف المرحلي إلى حالة الطاقة الكاملة. لقطع الطاقة بشكل كامل عن النظام، اضغط باستمرار زر التشغيل لمدة أربع ثوان.

إنذار: لا تستخدم زر التشغيل لإيقاف تشغيل الكمبيوتر إلا إذا توقف النظام عن الاستجابة؛ فقد يؤدي فصل الطاقة دون استجابة من قبل نظام التشغيل إلى إلحاق عطب بالبيانات الموجودة على القرص الثابت أو فقدانها.

موقع World Wide Web

يختبر مهندسو شركة HP بدقة البرامج التي تم تطويرها من قبل الشركة أو من قبل جهة خارجية ويصححون أية أخطاء فيها، كما يطورون برامج دعم خاصة بنظام التشغيل، وذلك لضمان أعلى مستوى من الأداء، والتوافق، والوثوقية لأجهزة كمبيوتر HP.

وعند التحول إلى أنظمة تشغيل جديدة أو مراجعة، فمن الهام جدا تطبيق برامج الدعم المصممة خصيصا لأنظمة التشغيل تلك. وإذا كنت تخطط لتشغيل إصدار من Microsoft Windows مختلف عن الإصدار المرفق بالكمبيوتر، فعليك تثبيت برامج تشغيل الأجهزة والأدوات المساعدة المناسبة للتأكد من اعتماد كافة الميزات وعملها بشكل صحيح.

وقد سهلت HP مهمة تحديد موقع برامج الدعم الأحدث، والوصول إليها، وتقييمها، وتثبيتها. يمكنك تحميل البرامج من الموقع http://www.hp.com/support.

يتضمن الموقع على ويب أحدث برامج تشغيل الأجهزة، والأدوات المساعدة، وصور ROM القابلة لإعادة البرمجة المطلوبة من أجل تشغيل أحدث إصدار لنظام التشغيل Microsoft Windows على جهاز كمبيوتر HP.

التجمعات والشركاء

تتكامل حلول الإدارة في HP مع تطبيقات أخرى لإدارة النظام، وهي تستند إلى المقاييس الصناعية، مثل:

- Desktop Management Interface (DMI) 2.0
- Wake on LAN Technology
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) support

تعقب الموجودات وحمايتها

توفر ميزات تعقب الموجودات المضمنة في الكمبيوتر، بيانات هامة حول تعقب الموجودات التي يمكن إدارتها باستخدام منتجات HP Insight Manager، أو HP Client Manager أو تطبيقات أخرى لإدارة النظام. ومنتجات Management Solutions Partners. ويمكنك الدمج التلقائي لميزات تعقب الموجودات وهذه المنتجات من اختيار أداة الإدارة الأفضل ملاءمة لبيئتك ومن زيادة فعالية استثماراتك في الأدوات الموجودة.

كما تقدم HP عدة حلول للتحكم بالوصول إلى المكونات والمعلومات القيمة. وتمنع ProtectTools Embedded Security، في حال تثبيتها، الوصول غير المصرح به إلى البيانات وتدقق في وحدة النظام وتصادق على مستخدمين خارجيين يحاولون الوصول إلى النظام. وتساعد ميزات الحماية مثل ProtectTools، وSmart Cover Sensor وSmart Cover Lock، المتوفرة في طرازات مختارة، على منع الوصول غير المصرح به إلى مكونات الكمبيوتر الداخلية. يمكنك حماية البيانات القيمة الموجودة من خلال تعطيل المنافذ التسلسلية، أو المتوازية، أو منافذ USB، أو تعطيل قدرات التمهيد بواسطة الوسائط القابلة للإخراج. يمكن توجيه تنبيهات Memory Change وSmart Cover Sensor تلقائيا إلى تطبيقات إدارة النظام لتسليم إعلام سريع حول وجود عبث في مكونات الكمبيوتر الداخلية.

تتوفر الخيارات ProtectTools، وSmart Cover Sensor وSmart Cover Lock في بعض الأنظمة المختارة.

استخدم الأدوات المساعدة التالية من أجل إدارة إعدادات الحماية على أجهزة كمبيوتر HP:

- محليا، باستخدام الأدوات المساعدة Computer Setup Utilities. انظر *دليل الأداة المساعدة لإعداد الكمبيوتر (F10)* الذي يصحب الكمبيوتر للحصول على مزيد من المعلومات والإرشادات حول استخدام Computer Setup Utilities.
- عن بعد، باستخدام HP Client Manager أو System Software Manager. يمكن هذا البرنامج النشر المتناسق والآمن والتحكم بإعدادات الحماية من خلال أداة بسيطة تشغل من سطر الأوامر.

يشير الجدول والمقاطع التالية إلى إدارة ميزات حماية الكمبيوتر محليا بواسطة الأدوات المساعدة Computer Setup (F10) Utilities.

نظرة عامة حول ميزات الحماية

الميزة	الغرض	كيفية تأسيسها
Removable Media Boot Control	منع التمهيد من محركات الأقراص القابلة للإخراج. (متوفرة في محركات أقراص مختارة)	من قائمة Computer Setup (F10) Utilities.
Serial, Parallel, USB, or Infrared Interface Control	منع نقل البيانات عبر الواجهات التسلسلية، أو المتوازية، أو منفذ USB (الناقل التسلسلي العالمي)، أو منفذ الأشعة تحت الحمراء.	من قائمة Computer Setup (F10) Utilities.
Power-On Password	منع استخدام الكمبيوتر إلى حين إدخال كلمة المرور. يمكن تطبيقه على بدء التشغيل الأولي للكمبيوتر وعلى إعادة التشغيل.	من قائمة Computer Setup (F10) Utilities.
Setup Password	منع إعادة تكوين الكمبيوتر (استخدام Computer Setup Utilities) إلى حين إدخال كلمة المرور.	من قائمة Computer Setup (F10) Utilities.
Embedded Security Device	منع الوصول غير المصرح به إلى البيانات باستخدام التشفير والحماية بواسطة كلمة المرور. التدقيق في وحدة النظام والمصادقة على مستخدمين خارجيين يحاولون الوصول إلى النظام.	من قائمة Computer Setup (F10) Utilities.
DriveLock	منع الوصول غير المصرح به إلى البيانات الموجودة على محركات أقراص ثابتة للحجرة المتعددة الأغراض. تتوفر هذه الميزة في طرازات مختارة فقط.	من قائمة Computer Setup (F10) Utilities.

✎ للحصول على المزيد من المعلومات حول Computer Setup، راجع *دليل الأداة المساعدة لإعداد الكمبيوتر (F10)*. قد يختلف اعتماد ميزات الحماية استنادا إلى التكوين الخاص بالكمبيوتر.

يتبع

نظرة عامة حول ميزات الحماية *(تتمة)*

الميزة	الغرض	كيفية تأسيسها
Smart Cover Sensor	الإشارة إلى نزع غطاء الكمبيوتر أو لوحته الجانبية. يمكن إعداده بحيث يتطلب كلمة مرور الإعداد لإعادة تشغيل الكمبيوتر، بعد نزع الغطاء أو اللوحة الجانبية للكمبيوتر. يرجى مراجعة الدليل المرجع للأجهزة الموجود على القرص المضغوط *Documentation Library* للحصول على مزيد من المعلومات حول هذه الميزة. هذه الميزة تتوفر في طرازات مختارة فقط.	من قائمة Computer Setup (F10) Utilities.
Master Boot Record Security	المنع المحتمل لإجراء تغييرات ضارة أو غير مقصودة على Master Boot Record الخاص بالقرص الحالي القابل للتمهيد، وتوفير وسيلة لاسترداد "آخر تكوين صالح معروف" من MBR.	من قائمة Computer Setup (F10) Utilities.
Memory Change Alerts	كشف تاريخ ووقت إضافة وحدات الذاكرة، أو نقلها، أو إزالتها؛ وإعلام المستخدم والمسؤول عن النظام.	للحصول على معلومات حول تمكين تنبيهات تغييرات الذاكرة، راجع *Intelligent Manageability Guide* عبر الإنترنت.

✎ للحصول على المزيد من المعلومات حول Computer Setup، راجع *دليل الأداة المساعدة لإعداد الكمبيوتر (F10)*. قد يختلف اعتماد ميزات الحماية استنادا إلى التكوين الخاص بالكمبيوتر.

يتبع

نظرة عامة حول ميزات الحماية *(تتمة)*

الميزة	الغرض	كيفية تأسيسها
Ownership Tag	عرض معلومات الملكية، كما تم تعريفها من قبل المسؤول عن النظام، أثناء عملية بدء تشغيل النظام (محمية بواسطة كلمة مرور الإعداد).	من قائمة Computer Setup Utilities (F10).
Cable Lock Provision	منع الوصول إلى داخل الكمبيوتر وذلك لتفادي حدوث تغييرات غير مرغوب بها في التكوين أو إخراج أحد المكونات. ويمكن استخدامه لإحكام ربط الكمبيوتر بجسم ثابت لمنع سرقته.	تثبيت قفل كبل لإحكام ربط الكمبيوتر بجسم ثابت.
Security Loop Provision	منع الوصول إلى داخل الكمبيوتر وذلك لتفادي حدوث تغييرات غير مرغوب بها في التكوين أو إخراج أحد المكونات.	تثبيت قفل في حلقة الحماية security loop لتفادي حدوث تغييرات غير مرغوب بها في التكوين أو إخراج أحد المكونات.

✎ للحصول على المزيد من المعلومات حول Computer Setup، راجع *دليل الأداة المساعدة لإعداد الكمبيوتر (F10)*. قد يختلف اعتماد ميزات الحماية استنادا إلى التكوين الخاص بالكمبيوتر.

الحماية بواسطة كلمة مرور

تمنع كلمة مرور بدء التشغيل الاستخدام غير المصرح به للكمبيوتر وذلك بطلب كلمة مرور لتمكين الوصول إلى التطبيقات أو البيانات في كل مرة يتم فيها تشغيل الكمبيوتر أو إعادة تشغيله. أما كلمة مرور الإعداد فتمنع بشكل خاص الوصول غير المصرح به إلى Computer Setup، ويمكن استخدامها لتجاوز كلمة مرور بدء التشغيل. وبمعنى آخر، فإن إدخال كلمة مرور الإعداد عوضا عن كلمة مرور بدء التشغيل عند مطالبتك بها، يسمح لك بالوصول إلى الكمبيوتر.

وبالإمكان إنشاء كلمة مرور الإعداد على مستوى شبكة الاتصال لتمكين المسؤول عن النظام من تسجيل الدخول إلى كافة أجهزة الكمبيوتر المتصلة بالشبكة للقيام بأعمال الصيانة دون الحاجة إلى معرفة كلمة مرور بدء التشغيل، حتى ولو كان قد تم إنشاء مثل هذه الكلمة.

إنشاء كلمة مرور الإعداد باستخدام Computer Setup

إذا كان النظام مجهزا بجهاز حماية مضمنة، فيمكنك الرجوع إلى "الحماية المضمنة" على الصفحة ٣٠.

يؤدي إنشاء كلمة مرور الإعداد بواسطة Computer Setup إلى منع إعادة تكوين الكمبيوتر (استخدام الأداة المساعدة Computer Setup (**F10**) إلى حين إدخال كلمة المرور.

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security**، ثم **Setup Password** واتبع الإرشادات التي تظهر على الشاشة.

٤. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

إنشاء كلمة مرور بدء التشغيل باستخدام Computer Setup

يؤدي إنشاء كلمة مرور بدء التشغيل بواسطة Computer Setup إلى منع الوصول إلى الكمبيوتر عند تشغيل الطاقة، إلا في حال إدخال كلمة المرور. عندما تكون كلمة مرور بدء التشغيل معينة، يعرض Computer Setup خيار Password Options ضمن قائمة Security. وتشمل خيارات كلمة المرور Password Prompt on Warm Boot. وعند تمكين تشغيل الخيار Password Prompt on Warm Boot، يجب أيضا أن يتم إدخال كلمة المرور في كل مرة يعاد فيها تمهيد الكمبيوتر.

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security**، ثم **Power-on Password** واتبع الإرشادات التي تظهر على الشاشة.

٤. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

إدخال كلمة مرور بدء التشغيل

لإدخال كلمة مرور بدء التشغيل، أكمل الخطوات التالية:

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. عندما يظهر رمز المفتاح على الشاشة، اكتب كلمة المرور الحالية، ثم اضغط المفتاح **Enter**.

✎ اكتب بعناية؛ فالأحرف التي تكتبها لن تظهر على الشاشة للمحافظة على سرية كلمة المرور.

إذا أدخلت كلمة المرور بشكل غير صحيح، فسيظهر رمز مفتاح مكسور. حاول مرة أخرى. وبعد ثلاث محاولات غير ناجحة، عليك إيقاف تشغيل الكمبيوتر، ثم تشغيله من جديد كي تتمكن من المتابعة.

إدخال كلمة مرور الإعداد

إذا كان النظام مجهزا بجهاز حماية مضمنة، فيمكنك الرجوع إلى "الحماية المضمنة" على الصفحة ٣٠.

إذا كان قد تم إنشاء كلمة مرور الإعداد على الكمبيوتر، فستتم مطالبتك بإدخالها في كل مرة تقوم فيها بتشغيل Computer Setup.

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. عندما يظهر رمز المفتاح على الشاشة، اكتب كلمة المرور الحالية، ثم اضغط المفتاح **Enter**.

اكتب بعناية؛ فالأحرف التي تكتبها لن تظهر على الشاشة للمحافظة على سرية كلمة المرور.

إذا أدخلت كلمة المرور بشكل غير صحيح، فسيظهر رمز مفتاح مكسور. حاول مرة أخرى. وبعد ثلاث محاولات غير ناجحة، عليك إيقاف تشغيل الكمبيوتر، ثم تشغيله من جديد كي تتمكن من المتابعة.

تغيير كلمة مرور بدء التشغيل أو كلمة مرور الإعداد

إذا كان النظام مجهزا بجهاز حماية مضمنة، فيمكنك الرجوع إلى "الحماية المضمنة" على الصفحة ٣٠.

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**. لتغيير كلمة مرور الإعداد، شغل **Computer Setup**.

٢. عندما يظهر رمز المفتاح، اكتب كلمة المرور الحالية، ثم خطا مائلا (/) أو الحرف المحدد البديل، ثم كلمة المرور الجديدة، ثم خطا مائلا آخر (/) أو الحرف المحدد البديل وكلمة المرور الجديدة مرة أخرى على الشكل التالي:
current password/new password/new password

اكتب بعناية؛ فالأحرف التي تكتبها لن تظهر على الشاشة للمحافظة على سرية كلمة المرور.

---

٣. اضغط المفتاح **Enter**.

تدخل كلمة المرور الجديدة حيز التنفيذ في المرة التالية التي تشغل فيها الكمبيوتر.

راجع المقطع "الأحرف المحددة في لوحة المفاتيح المحلية" على الصفحة ٢٩ للحصول على معلومات حول الأحرف المحددة البديلة. يمكنك أيضا تغيير كلمة مرور الإعداد وكلمة مرور بدء التشغيل باستخدام Security Options في Computer Setup.

حذف كلمة مرور بدء التشغيل أو كلمة مرور الإعداد

إذا كان النظام مجهزا بجهاز حماية مضمنة، فيمكنك الرجوع إلى "الحماية المضمنة" على الصفحة ٣٠.

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**. لحذف كلمة مرور الإعداد، شغل **Computer Setup**.

٢. عندما يظهر رمز المفتاح، اكتب كلمة المرور الحالية يتبعها خط مائل (/) أو الحرف المحدد البديل على الشكل التالي:
current password/

٣. اضغط المفتاح **Enter**.

راجع المقطع "الأحرف المحددة في لوحة المفاتيح المحلية" في هذا الفصل للحصول على معلومات حول الأحرف المحددة البديلة. يمكنك أيضا تغيير كلمة مرور الإعداد وكلمة مرور بدء التشغيل باستخدام Security Options في Computer Setup.

الأحرف المحددة في لوحة المفاتيح المحلية

لقد تم تصميم كل لوحة من لوحات المفاتيح بحيث تفي بالمتطلبات الخاصة بكل بلد. فبناء الجملة والمفاتيح التي تستخدمها لتغيير كلمة المرور أو حذفها تتوقف على لوحة المفاتيح التي تصحب الكمبيوتر.

الأحرف المحددة في لوحة المفاتيح المحلية

الألمانية	-	التايلاندية	/	العربية	/
الأميركية اللاتينية	-	التركية	.	الفرنسية	!
الإسبانية	-	التشيكية	-	الفرنسية الكندية	é
الإنكليزية – المملكة المتحدة	/	الدانمركية	-	الكورية	/
الإنكليزية – الولايات المتحدة	/	الروسية	/	النرويجية	-
الإيطالية	-	السلوفاكية	-	الهنغارية	-
البرازيلية	/	السويدية – فنلندة	/	اليابانية	/
البرتغالية	-	السويسرية	-	اليونانية	-
البلجيكية	=	الصينية	/	BHCSY *	-
البولندية	-	العبرية	.		

* للبوسنة والهرسك، وكرواتيا، وسلوفينيا، ويوغسلافيا

مسح كلمات المرور

إذا نسيت كلمة المرور، فلن تتمكن من تشغيل الكمبيوتر. ويمكنك الرجوع إلى *دليل استكشاف الأخطاء وإصلاحها* للحصول على معلومات حول كيفية مسح كلمات المرور.

إذا كان النظام مجهزا بجهاز حماية مضمنة، فيمكنك الرجوع إلى "الحماية المضمنة".

الحماية المضمنة

تدمج الحماية المضمنة بواسطة أدوات الحماية ProtectTools Embedded Security التشفير والحماية بواسطة كلمة مرور لتوفير الحماية المحسنة لتشفير الملفات/المجلدات في نظام الملفات المضمن (EFS) وحماية البريد الإلكتروني في Microsoft Outlook وOutlook Express. وتتوفر أدوات الحماية ProtectTools لأجهزة كمبيوتر مكتبية للأعمال محددة كخيارات Configured-To-Order (CTO). وهي موجهة لعملاء HP الذين تشكل حماية البيانات أولى اهتماماتهم: فالوصول غير المصرح به إلى البيانات يمثل خطرا يفوق خطر فقدان البيانات. وتستخدم أدوات الحماية ProtectTools أربع كلمات مرور:

- Setup (F10) — للدخول إلى Computer Setup (F10) Utility وتمكين/تعطيل تشغيل ProtectTools
- Take Ownership — يتم تعيينها واستخدامها من قبل المسؤول عن النظام، الذي يصرح للمستخدمين ويعين معلمات الحماية
- Emergency Recovery Token — يتم تعيينها من قبل المسؤول عن النظام، وتسمح باسترداد النظام في حال حدوث عطل في رقاقة ProtectTools
- Basic User — يتم تعيينها واستخدامها من قبل المستخدم

إذا فقدت كلمة مرور المستخدم، فسيتعذر استرداد البيانات المشفرة. وبالتالي، فإن استخدام ProtectTools يكون أكثر أمانا عند إجراء نسخ متطابق للبيانات الموجودة في محرك أقراص المستخدم على نظام معلومات النظام أو إذا كان يتم إجراء نسخ احتياطي لها بشكل دوري.

إن ProtectTools Embedded Security عبارة عن رقاقة حماية متوافقة مع TCPA 1.1 يتم تثبيتها بشكل اختياري على لوحة النظام في أجهزة كمبيوتر مكتبية للأعمال محددة. وتعتبر كل رقاقة ProtectTools Embedded Security فريدة ويتم ربطها بجهاز كمبيوتر معين. وتقوم كل رقاقة بتنفيذ عمليات حماية رئيسية بشكل مستقل عن مكونات الكمبيوتر الأخرى (مثل المعالج، أو الذاكرة، أو نظام التشغيل).

جهاز الكمبيوتر الذي تم تمكينه لاستخدام ProtectTools Embedded Security يقوم بتكملة وتحسين قدرات الحماية الكامنة في Microsoft Windows 2000 أو Windows XP Professional أو Home Edition. ففيما يستطيع نظام التشغيل مثلا تشفير الملفات والمجلدات المحلية استنادا إلى EFS، فإن ProtectTools Embedded Security تقدم طبقة إضافية من الحماية وذلك بإنشاء مفاتيح تشفير من المفتاح الجذر للنظام الأساسي (المخزن في سيليكون). هذه العملية تعرف بـــ "تغليف" مفاتيح التشفير. ولا تمنع أدوات الحماية ProtectTools الوصول إلى الشبكة من قبل كمبيوتر لا تتوفر فيه هذه الأدوات.

القدرات الرئيسية لـــ ProtectTools Embedded Security تشمل:

- مصادقة على النظام الأساسي
- تخزين محمي
- وحدة البيانات

إنذار: عليك حماية كلمات المرور. **لا يمكن الوصول إلى البيانات المشفرة أو استردادها دون كلمات المرور.**

إعداد كلمات المرور

الإعداد

يمكن إنشاء كلمة مرور الإعداد وتمكين تشغيل جهاز الحماية المضمنة بواسطة الأداة المساعدة F10 setup.

١. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

٢. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل لتحديد لغة، ثم اضغط **Enter**.

٣. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى علامة التبويب **Security**، ثم استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Setup Password**. اضغط **Enter**.

٤. اكتب كلمة مرور وأكدها. اضغط **F10** لقبول كلمة المرور.

اكتب بعناية؛ الأحرف التي تكتبها لا تظهر على الشاشة وذلك لأسباب تتعلق بالحماية.

٥. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Embedded Security Device**. اضغط **Enter**.

٦. إذا كان الخيار المحدد في مربع الحوار هو —**Embedded Security Device Disable**، فاستخدم مفتاح السهم إلى اليسار أو إلى اليمين للتغيير إلى **Embedded Security Device—Enable**. اضغط **F10** لقبول التغيير.

إنذار: إذا حددت **Reset to Factory Settings—Reset**، فسيتم مسح كافة المفاتيح وسيتعذر استرداد البيانات المشفرة ما لم يتم إجراء نسخ احتياطي للمفاتيح (انظر "Take Ownership and Emergency Recovery Token".) حدد **Reset** فقط عندما يتم إعلامك بالقيام بذلك في الإجراء المتعلق باسترداد البيانات المشفرة (انظر "استرداد البيانات المشفرة" على الصفحة ٣٥).

٧. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى File. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Save Changes and Exit**. اضغط **Enter**، ثم اضغط **F10** للتأكيد.

Take Ownership و Emergency Recovery Token

كلمة المرور Take Ownership مطلوبة لتمكين أو تعطيل النظام الأساسي وللتصريح للمستخدمين. وإذا فشل جهاز الحماية المضمنة، فإن آلية Emergency Recovery تسمح بالتصريح للمستخدمين وبالوصول إلى البيانات.

١. إذا كنت تستخدم Windows XP Professional أو Home Edition، فانقر فوق **Start > All Programs > HP ProtectTools Embedded Security > Tools > Embedded Security Initialization Wizard**.

إذا كنت تستخدم Windows 2000، فانقر فوق **Start > Programs > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

٢. انقر فوق **Next**.

٣. اكتب كلمة مرور Take Ownership وقم بتأكيدها، ثم انقر فوق **Next**.

اكتب بعناية؛ فالأحرف التي تكتبها لا تظهر على الشاشة وذلك لأسباب تتعلق بالحماية.

٤. انقر فوق **Next** لقبول موقع الأرشيف الافتراضي للاسترداد.

٥. اكتب كلمة مرور Emergency Recovery Token وقم بتأكيدها، ثم انقر فوق **Next**.

٦. أدخل قرصا مرنا لتخزين Emergency Recovery Token Key. انقر فوق **Browse** وحدد القرص المرن.

إنذار: يستخدم Emergency Recovery Token Key لاسترداد البيانات المشفرة في حال حدوث عطل في الكمبيوتر أو في رقاقة الحماية المضمنة. **ولا يمكن استرداد البيانات دون المفتاح.** (لا يمكن الوصول إلى البيانات دون كلمة المرور Basic User.) وعليك تخزين هذا القرص المرن في مكان آمن.

٧. انقر فوق **Save** لقبول الموقع واسم الملف الافتراضي، ثم انقر فوق **Next**.

٨. انقر فوق **Next** لتأكيد الإعدادات قبل أن تتم تهيئة Security Platform.

قد تظهر رسالة تفيد بعدم تهيئة ميزات الحماية المضمنة Embedded Security. لا تنقر في الرسالة؛ فسيتم معالجة الأمر في وقت لاحق في الإجراء وستغلق الرسالة بعد بضع ثوان.

٩. انقر فوق **Next** لتجاوز تكوين النهج المحلية.

١٠. تأكد من تحديد خانة الاختيار Start Embedded Security User Initialization Wizard، ثم انقر فوق **Finish**.

فيبدأ الآن تلقائيا تشغيل User Initialization Wizard.

Basic User

يتم إنشاء كلمة المرور Basic User أثناء التهيئة من قبل المستخدم. كلمة المرور هذه مطلوبة لإدخال البيانات المشفرة والوصول إليها.

إنذار: عليك حماية كلمة المرور Basic User. **لا يمكن الوصول إلى البيانات المشفرة أو استردادها دون كلمة المرور هذه.**

١. إذا لم يكن المعالج User Initialization Wizard مفتوحا:

إذا كنت تستخدم Windows XP Professional أو Home Edition، فانقر فوق **Start > All Programs > HP ProtectTools Embedded Security > Tools > User Initialization Wizard**.

إذا كنت تستخدم Windows 2000، فانقر فوق **Start > Programs > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

٢. انقر فوق **Next**.

٣. اكتب كلمة مرور Basic User Key وقم بتأكيدها، ثم انقر فوق **Next**.

اكتب بعناية؛ فالأحرف التي تكتبها لا تظهر على الشاشة وذلك لأسباب تتعلق بالحماية.

٤. انقر فوق **Next** لتأكيد الإعدادات.

٥. حدد ميزات الحماية (Security Features) المناسبة وانقر فوق **Next**.

٦. انقر فوق عميل البريد الإلكتروني المناسب لتحديده، ثم انقر فوق **Next**.

٧. انقر فوق **Next** لتطبيق شهادة التشفير Encryption Certificate.

٨. انقر فوق **Next** لتأكيد الإعدادات.

٩. انقر فوق **Finish**.

١٠. أعد تشغيل الكمبيوتر.

استرداد البيانات المشفرة

لاسترداد البيانات بعد استبدال رقاقة ProtectTools، يجب أن يتوفر لديك ما يلي:

- SPEmRecToken.xml — وهو Emergency Recovery Token Key
- SPEmRecArchive.xml — ملف مخفي، الموقع الافتراضي:
  C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- كلمات مرور ProtectTools
  - ❑ Setup
  - ❑ Take Ownership
  - ❑ Emergency Recovery Token
  - ❑ Basic User

١. أعد تشغيل الكمبيوتر.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** مرة أخرى للوصول إلى الأداة المساعدة.

---

٣. اكتب كلمة مرور Setup، ثم اضغط **Enter**.

٤. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل لتحديد لغة، ثم اضغط **Enter**.

٥. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى علامة التبويب **Security**، ثم استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Embedded Security Device**. اضغط **Enter**.

٦. في حال توفر تحديد واحد فقط **Embedded Security Device—Disable**:

أ. استخدم مفتاح السهم إلى اليسار أو إلى اليمين لتغيير التحديد إلى **Embedded Security Device—Enable**. اضغط **F10** لقبول التغيير.

ب. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى **File**. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Save Changes and Exit**. اضغط **Enter**، ثم اضغط **F10** للتأكيد.

ت. انتقل إلى الخطوة ١.

في حال توفر تحديدين، انتقل إلى الخطوة ٧.

٧. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Reset to Factory Settings—Do Not Reset**. اضغط مفتاح السهم إلى اليسار أو إلى اليمين.

تظهر رسالة تفيد بما يلي: Performing this action will reset the embedded security device to factory settings if settings are saved on exit. اضغط أي مفتاح للمتابعة.

اضغط **Enter**.

٨. التحديد يقرأ الآن على الشكل التالي **Reset to Factory Settings—Reset**. اضغط **F10** لقبول التغيير.

٩. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى **File**. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Save Changes and Exit**. اضغط **Enter**، ثم اضغط **F10** للتأكيد.

١٠. أعد تشغيل الكمبيوتر.

١١. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10 مرة أخرى** للوصول إلى الأداة المساعدة.

---

١٢. اكتب كلمة مرور Setup، ثم اضغط **Enter**.

١٣. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل لتحديد لغة، ثم اضغط **Enter**.

١٤. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى علامة التبويب **Security**، ثم استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Embedded Security Device**. اضغط **Enter**.

١٥. إذا كان التحديد في مربع الحوار هو **Embedded Security Device—Disable**، فاستخدم مفتاح السهم إلى اليسار أو إلى اليمين لتغيير التحديد إلى **Embedded Security Device—Enable**. اضغط **F10**.

١٦. استخدم مفتاح السهم إلى اليسار أو إلى اليمين للانتقال إلى **File**. استخدم مفتاح السهم إلى الأعلى أو إلى الأسفل للانتقال إلى **Save Changes and Exit**. اضغط **Enter**، ثم اضغط **F10** للتأكيد.

١٧. بعد أن يتم فتح Windows:

إذا كنت تستخدم Windows XP Professional أو Home Edition، فانقر فوق **HP ProtectTools Embedded Security < All Programs < Start** **.Embedded Security Initialization Wizard < Tools**

إذا كنت تستخدم Windows 2000، فانقر فوق **Start < Programs < HP ProtectTools Embedded Security Tools < Embedded** **.Security Initialization Wizard**

١٨. انقر فوق **Next**.

١٩. اكتب كلمة مرور Take Ownership وقم بتأكيدها، ثم انقر فوق **Next**.

اكتب بعناية؛ فالأحرف التي تكتبها لا تظهر على الشاشة وذلك لأسباب تتعلق بالحماية.

---

٢٠. تأكد من تحديد الخيار Create a new recovery archive. ضمن **Recovery archive location**، انقر فوق **Browse**.

٢١. لا تقبل اسم الملف الافتراضي. اكتب اسما جديدا للملف لتجنب استبدال الملف الأصلي.

٢٢. انقر فوق **Save**، ثم فوق **Next**.

٢٣. اكتب كلمة مرور Emergency Recovery Token وقم بتأكيدها، ثم انقر فوق **Next**.

٢٤. أدخل قرصا مرنا لتخزين Emergency Recovery Token Key عليه. انقر فوق **Browse** وحدد القرص المرن.

٢٥. لا تقبل اسم المفتاح الافتراضي. اكتب اسما جديدا للمفتاح لتجنب استبدال المفتاح الأصلي.

٢٦. انقر فوق **Save**، ثم فوق **Next**.

٢٧. انقر فوق **Next** لتأكيد الإعدادات قبل أن تتم تهيئة Security Platform.

قد تظهر رسالة تفيد بتعذر تحميل Basic User Key. لا تنقر في الرسالة؛ فسيتم معالجة الأمر في وقت لاحق في الإجراء وستغلق الرسالة بعد بضع ثوان.

---

٢٨. انقر فوق **Next** لتجاوز تكوين النهج المحلية.

٢٩. انقر لمسح خانة الاختيار **Start Embedded Security User Initialization Wizard**. انقر فوق **Finish**.

٣٠. انقر بزر الماوس الأيمن فوق الرمز ProtectTools في شريط الأدوات وانقر فوق **Initialize Embedded Security restoration**.

يؤدي هذا إلى بدء تشغيل HP ProtectTools Embedded Security Initialization Wizard.

٣١. انقر فوق **Next**.

٣٢. أدخل القرص المرن حيث تم تخزين Emergency Recovery Token Key الأصلي. انقر فوق **Browse**، ثم حدد موقع الرمز وانقر فوقه نقرا مزدوجا لإدخال الاسم في الحقل. الاسم الافتراضي هو A:\SPEmRecToken.xml.

٣٣. اكتب كلمة مرور Token الأصلية ثم انقر فوق **Next**.

٣٤. انقر فوق **Browse**، ثم حدد موقع أرشيف الاسترداد الأصلي وانقر فوقه نقرا مزدوجا لإدخال الاسم في الحقل. الموقع الافتراضي هو C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.

٣٥. انقر فوق **Next**.

٣٦. انقر فوق الجهاز الذي تريد استعادته وانقر فوق **Next**.

٣٧. انقر فوق **Next** لتأكيد الإعدادات.

٣٨. إذا أعلن المعالج عن استعادة النظام الأساسي للحماية، فانتقل إلى الخطوة ٣٩.

إذا أعلن المعالج فشل عملية الاستعادة، فعد إلى الخطوة ١٠. دقق بعناية في كلمات المرور، وكذلك في موقع الرمز واسمه، وموقع الأرشيف واسمه.

٣٩. انقر فوق **Finish**.

٤٠. إذا كنت تستخدم Windows XP Professional أو Home Edition، فانقر فوق **Start > All Programs > HP ProtectTools Embedded Security > Tools > User Initialization Wizard**.

إذا كنت تستخدم Windows 2000، فانقر فوق **Start > Programs > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

٤١. انقر فوق **Next**.

٤٢. انقر فوق **Recover your basic user key** وانقر فوق **Next**.

٤٣. حدد مستخدما، واكتب كلمة المرور Basic User Key الأصلية لذلك المستخدم، ثم انقر فوق **Next**.

٤٤. انقر فوق **Next** لتأكيد الإعدادات وقبول الموقع الافتراضي لبيانات الاسترداد.

الخطوات من ٤٥ إلى ٤٩ تعيد تثبيت تكوين Basic User الأصلي.

٤٥. حدد ميزات الحماية Security Features المناسبة وانقر فوق **Next**.

٤٦. انقر فوق عميل البريد الإلكتروني المناسب لتحديده، ثم انقر فوق **Next**.

٤٧. انقر فوق شهادة التشفير Encryption Certificate وانقر فوق **Next** لتطبيقها.

٤٨. انقر فوق **Next** لتأكيد الإعدادات.

٤٩. انقر فوق **Finish**.

٥٠. أعد تشغيل الكمبيوتر

إنذار: عليك حماية كلمة المرور Basic User. **لا يمكن الوصول إلى البيانات المشفرة أو استردادها دون كلمة المرور هذه.**

DriveLock

ميزة DriveLock عبارة عن ميزة حماية تخضع للمقاييس الصناعية تمنع الوصول غير المصرح به إلى البيانات الموجودة على محركات أقراص ثابتة للحجرة المتعددة الأغراض MultiBay. ميزة DriveLock مصممة كملحق لـــ Computer Setup. وتتوفر فقط عند الكشف عن محركات أقراص ثابتة تتمتع بخاصية DriveLock.

تتوفر ميزة DriveLock خصيصا لعملاء HP الذين تشكل حماية البيانات أولى اهتماماتهم. ولا تعتبر تكلفة محرك القرص الثابت وفقدان البيانات المخزنة عليه لمثل هؤلاء العملاء ذات أهمية بالغة مقارنة بالضرر الذي قد ينتج عن الوصول غير المصرح به لمحتوياته. ولموازنة هذا المستوى من الحماية مع الحاجة العملية للتعويض عن كلمة مرور منسية، يستخدم تطبيق HP لميزة DriveLock نظام حماية من كلمتي مرور. يتم تعيين إحدى كلمتي المرور واستخدامها من قبل المسؤول عن النظام، في حين يتم تعيين كلمة المرور الأخرى واستخدامها من قبل المستخدم. ولا يوجد هنا أي طريقة أخرى مخفية يمكن استخدامها لإلغاء قفل محرك الأقراص في حال فقدان كلمتي المرور. ولذلك، يمكن أن يكون استخدام DriveLock أكثر أمانا عند نسخ البيانات الموجودة على محرك القرص الثابت ووضعها على نظام معلومات الشركة (بواسطة النسخ المتماثل) أو عند نسخها احتياطيا بشكل منتظم.

في حال فقدان كلمتي مرور DriveLock، يصبح محرك القرص الثابت غير قابل للاستخدام. وقد تعتبر هذه مخاطرة غير مقبولة لأي مستخدم لا يطابق الوصف المعرف سابقا. أما بالنسبة للمستخدمين الذين يطابقون ذلك الوصف، فقد تكون هذه مخاطرة مقبولة وفقا لطبيعة البيانات المخزنة على محرك القرص الثابت.

استخدام DriveLock

يظهر الخيار DriveLock ضمن القائمة Security في Computer Setup. ويعرض على المستخدم خيارات لتعيين كلمة المرور الرئيسية أو لتمكين استخدام DriveLock. ويجب توفير كلمة مرور المستخدم لتمكين DriveLock. وبما أنه يتم إنجاز التكوين الأولي لـــ DriveLock عادة من قبل المسؤول عن النظام، فيجب تعيين كلمة المرور الرئيسية أولا. تشجع HP المسؤولين عن النظام على تعيين كلمة مرور رئيسية سواء رغبوا بتمكين استخدام ميزة DriveLock أو بالإبقاء عليه معطلا. هذا يعطي المسؤول إمكانية تعديل إعدادات DriveLock إذا ما أصبح محرك الأقراص مقفلا في المستقبل. وعند تعيين كلمة المرور الرئيسية، يمكن للمسؤول عن النظام تمكين استخدام DriveLock أو إبقاؤه معطلا.

عند وجود محرك قرص ثابت مقفل، يطلب الاختبار الذاتي للتشغيل (POST) كلمة مرور لإلغاء قفل الجهاز. إذا تم تعيين كلمة مرور بدء التشغيل وكانت مطابقة لكلمة مرور المستخدم الخاصة بالجهاز، فلن يطالب اختبار POST المستخدم بإعادة إدخال كلمة المرور. وإلا، فستتم مطالبة المستخدم بإدخال كلمة مرور DriveLock. يمكن استخدام كلمة مرور المستخدم أو كلمة المرور الرئيسية. وتتوفر للمستخدمين محاولتان لإدخال كلمة مرور صحيحة. إذا لم تنجح أي من المحاولتين، يستمر POST ولكن تبقى البيانات على محرك الأقراص غير قابلة للوصول إليها.

تطبيقات DriveLock

التطبيق العملي الأهم لميزة حماية DriveLock هو في إطار بيئة شركة حيث يوفر المسؤول عن النظام للمستخدمين محركات أقراص ثابتة خاصة بالحجر متعددة الأغراض للاستخدام في بعض أجهزة الكمبيوتر. يكون المسؤول عن النظام مسؤولا عن تكوين محرك القرص الثابت للحجرة متعددة الأغراض والذي قد يتضمن، بالإضافة إلى أشياء أخرى، إعداد كلمة المرور الرئيسية لـــ DriveLock. في حال نسيان المستخدم لكلمة مرور المستخدم أو نقل الجهاز إلى موظف آخر، يمكن استخدام كلمة المرور الرئيسية دوما لإعادة تعيين كلمة مرور المستخدم وإمكانية الوصول مجددا إلى محرك القرص الثابت.

تنصح HP أن يقوم المسؤولون عن النظام في الشركات والذين يختارون تمكين استخدام DriveLock، بإنشاء نهج للشركة أيضا من أجل إعداد كلمات المرور الرئيسية والمحافظة عليها. يجب القيام بهذا لمنع موظف ما من تعيين كلمتي مرور DriveLock عمدا أو عن غير قصد قبل تركه للشركة. في مثل هذه الحالة، يصبح محرك القرص الثابت غير قابل للاستخدام ويتوجب استبداله. إضافة إلى ذلك، فعند عدم تعيين كلمة مرور رئيسية، قد يجد المسؤولون عن النظام أنفسهم غير قادرين على الوصول إلى محرك القرص الثابت لإنجاز عمليات التدقيق الروتينية بحثا عن البرامج غير المرخصة، ووظائف التحكم بموجودات أخرى ودعمها.

لا تنصح HP المستخدمين ذوي متطلبات الحماية الأقل بتمكين استخدام DriveLock. تتضمن هذه الفئة المستخدمين الشخصيين أو المستخدمين الذين لا يحتفظون عادة، ببيانات حساسة على محركات الأقراص الثابتة الخاصة بهم. تكون قيمة الفقدان المحتمل لمحرك الأقراص نتيجة لنسيان كلمتي المرور بالنسبة لهؤلاء المستخدمين أكبر بكثير من قيمة البيانات التي تم تعيين DriveLock من أجل حمايتها. يمكن تقييد الوصول إلى Computer Setup وDriveLock من خلال كلمة مرور الإعداد. عن طريق تعيين كلمة مرور الإعداد وعدم إعطائها للمستخدمين، يمكن للمسؤولين عن النظام منع المستخدمين من تمكين استخدام DriveLock.

متحسس الغطاء Smart Cover Sensor

يتوفر متحسس الغطاء Smart Cover Sensor في طرازات مختارة فقط، وهو عبارة عن مزيج من تقنية الأجهزة والبرامج يمكنه تنبيهك عندما يتم رفع غطاء الكمبيوتر أو لوحة تغطيته الجانبية. وهناك ثلاثة مستويات للحماية، كما هو موضح في الجدول التالي:

مستويات حماية Smart Cover Sensor

المستوى	الإعداد	الوصف
Level 0	Disabled	تعطيل استخدام Smart Cover Sensor (الإعداد الافتراضي).
Level 1	Notify User	عند إعادة تشغيل الكمبيوتر، يتم عرض رسالة على الشاشة تشير إلى أنه قد تم رفع غطاء الكمبيوتر أو لوحة تغطيته الجانبية.
Level 2	Setup Password	عند إعادة تشغيل الكمبيوتر، يتم عرض رسالة على الشاشة تشير إلى أنه قد تم رفع غطاء الكمبيوتر أو لوحة تغطيته الجانبية. في هذه الحالة، يجب إدخال كلمة مرور الإعداد من أجل المتابعة.

✎ بالإمكان تغيير هذه الإعدادات باستخدام Computer Setup. للحصول على مزيد من المعلومات حول Computer Setup، انظر *دليل الأداة المساعدة لإعداد الكمبيوتر (F10)*.

تعيين مستوى حماية Smart Cover Sensor

لتعيين مستوى حماية Smart Cover Sensor، أكمل الخطوات التالية:

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** مرة أخرى للوصول إلى الأداة المساعدة.

---

٢. حدد **Security**، ثم **Smart Cover** واتبع الإرشادات التي تظهر على الشاشة.

٣. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

Smart Cover Lock

Smart Cover Lock عبارة عن قفل للغطاء يتم التحكم به بواسطة برنامج، وهذه الميزة موجودة في أجهزة كمبيوتر مختارة من HP. ويمنع هذا القفل الوصول غير المصرح به إلى المكونات الداخلية. وعند شراء أجهزة الكمبيوتر، يكون Smart Cover Lock في وضع "الفتح".

إنذار: للحصول على أقصى درجة الحماية بواسطة قفل الغطاء، تأكد من تعيين كلمة مرور الإعداد. فكلمة مرور الإعداد تمنع الوصول غير المصرح به إلى الأداة المساعدة Computer Setup.

يتوفر Smart Cover Lock كخيار في بعض الأنظمة المختارة.

إقفال Smart Cover Lock

لتنشيط وإقفال Smart Cover Lock، أكمل الخطوات التالية:

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security**، ثم **Smart Cover** والخيار **Locked**.

٤. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

إلغاء إقفال Smart Cover Lock

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security > Smart Cover > Unlocked**.

٤. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

استخدام Smart Cover FailSafe Key

إذا قمت بتمكين استخدام Smart Cover Lock ولم تعد قادرا على إدخال كلمة المرور لتعطيل القفل، سوف تحتاج إلى مفتاح Smart Cover FailSafe Key لفتح غطاء الكمبيوتر. وتحتاج إلى المفتاح في أي من الظروف التالية:

- انقطاع التيار الكهربائي
- فشل بدء التشغيل
- فشل أحد مكونات الكمبيوتر (المعالج أو وحدة التزويد بالطاقة)
- نسيان كلمة المرور

إنذار: مفتاح Smart Cover FailSafe Key هو أداة تخصصية توفرها HP. كن جاهزا للطوارئ؛ اطلب هذا المفتاح قبل أن تحتاج إليه من معيد بيع أو موفر خدمات معتمد.

للحصول على FailSafe Key، يجب القيام بأحد الإجراءات التالية:

- الاتصال بمعيد بيع أو موفر خدمات.
- الاتصال بالرقم المناسب المذكور في الكفالة.

للحصول على مزيد من المعلومات حول استخدام Smart Cover FailSafe Key، يمكنك مراجعة *الدليل المرجع للأجهزة*.

حماية سجل التمهيد الرئيسي Master Boot Record Security

يحتوي سجل التمهيد الرئيسي Master Boot Record (MBR) على المعلومات المطلوبة لنجاح التمهيد من القرص والوصول إلى البيانات المخزنة على القرص. قد يمنع برنامج Master Boot Record Security حدوث تغييرات غير مقصودة أو خطيرة على MBR، مثل التغييرات الناتجة عن بعض فيروسات الكمبيوتر أو التغييرات الناتجة عن الاستخدام غير الصحيح لأدوات معينة من الأدوات المساعدة للقرص. ويسمح لك أيضا باسترداد "آخر سجل MBR صالح معروف" عند الكشف عن حصول تغييرات في MBR عند إعادة تشغيل النظام.

لتمكين استخدام MBR Security، نفذ الخطوات التالية:

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10 مرة أخرى** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security > Master Boot Record Security > Enabled**.

٤. حدد **Security > Save Master Boot Record> Enabled**.

٥. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

عندما يكون استخدام MBR Security ممكنا، يمنع BIOS حدوث أي تغييرات على سجل MBR للقرص الحالي القابل للتمهيد أثناء تشغيل النظام في وضع MS-DOS أو في Windows Safe Mode.

✎ تتحكم معظم أنظمة التشغيل بالوصول إلى سجل MBR للقرص الحالي القابل للتمهيد؛ وبذلك لا يتمكن BIOS من منع التغييرات التي قد تحدث أثناء عمل نظام التشغيل.

في كل مرة يتم فيها تشغيل الكمبيوتر أو إعادة تشغيله، يقارن BIOS بين سجل MBR للقرص الحالي القابل للتمهيد وسجل MBR المخزن مسبقا. إذا تم الكشف عن تغييرات وكان القرص الحالي القابل للتمهيد هو القرص نفسه الذي تم تخزين MBR مسبقا منه، فيتم عرض الرسالة التالية:

1999—Master Boot Record has changed.

Press any key to enter Setup to configure MBR Security.

عند الدخول إلى Computer Setup، يجب

- حفظ سجل MBR للقرص الحالي القابل للتمهيد؛ أو
- استرداد سجل MBR المخزن مسبقا؛ أو
- تعطيل ميزة MBR Security.

يجب أن تكون على علم بكلمة مرور الإعداد، في حال وجودها.

إذا تم الكشف عن تغييرات وكان القرص الحالي القابل للتمهيد **ليس** القرص نفسه الذي تم حفظ سجل MBR منه مسبقا، فيتم عرض الرسالة التالية:

2000—Master Boot Record Hard Drive has changed.

Press any key to enter Setup to configure MBR Security.

عند الدخول إلى Computer Setup، يجب

- حفظ سجل MBR للقرص الحالي القابل للتمهيد؛ أو
- تعطيل ميزة MBR Security.

يجب أن تكون على علم بكلمة مرور الإعداد، في حال وجودها.

في حال حدوث تلف غير متوقع في سجل MBR المخزن مسبقا، فيتم عرض الرسالة التالية:

1998—Master Boot Record has been lost.

Press any key to enter Setup to configure MBR Security.

عند الدخول إلى Computer Setup، يجب

- حفظ سجل MBR للقرص الحالي القابل للتمهيد؛ أو
- تعطيل ميزة MBR Security.

يجب أن تكون على علم بكلمة مرور الإعداد، في حال وجودها.

قبل تجزئة القرص الحالي القابل للتمهيد أو تهيئته

تأكد من تعطيل استخدام MBR Security قبل تغيير تجزئة أو تهيئة القرص الحالي القابل للتمهيد. تحاول بعض الأدوات المساعدة للقرص، مثل FDISK وFORMAT، تحديث MBR. في حال تمكين استخدام MBR Security عند تغيير تجزئة القرص أو تهيئته، فقد تتلقى رسائل إعلام بالخطأ من الأداة المساعدة للقرص أو قد تتلقى تحذيرا من MBR Security وذلك في المرة التالية التي يتم فيها تشغيل الكمبيوتر أو إعادة تشغيله. لتعطيل استخدام MBR Security، نفذ الخطوات التالية:

١. شغل الكمبيوتر أو أعد تشغيله. إذا كنت ضمن Windows، فانقر فوق **Start > Shut Down > Restart the Computer**.

٢. اضغط المفتاح **F10** عندما يتحول ضوء الشاشة إلى أخضر. اضغط **Enter** لتجاوز شاشة العنوان، إذا اقتضى الأمر ذلك.

✎ إذا لم تضغط المفتاح **F10** في الوقت المناسب، فعليك إيقاف تشغيل الكمبيوتر، ثم إعادة تشغيله، وضغط المفتاح **F10** للوصول إلى الأداة المساعدة.

---

٣. حدد **Security > Master Boot Record Security > Disabled**.

٤. قبل الإنهاء، انقر فوق **File > Save Changes and Exit**.

قفل الكبل

بالإمكان توصيل قفل الكبل بلوحة الكمبيوتر الخلفية بحيث يمكن إحكام تثبيت الكمبيوتر بشكل فعلي عن طريق ربطه بمنطقة العمل المحيطة به.

للحصول على إرشادات مصورة، الرجاء مراجعة *الدليل المرجع للأجهزة* الموجود على القرص المضغوط *Documentation Library*.

تقنية التعرف على بصمات الأصابع Fingerprint Identification Technology

تزيد تقنية التعرف على بصمات الأصابع من HP Fingerprint Identification Technology، من حماية شبكة الاتصال، وتبسط عملية تسجيل الدخول، وتخفض التكاليف المقترنة بإدارة شبكات اتصال الشركات، وذلك بإلغاء الحاجة لإدخال كلمة مرور المستخدم. نتيجة لتدني تكاليفها، لم تعد هذه الميزة مخصصة فقط للمؤسسات ذات التقنيات العالية والتي تتطلب مستوى مرتفعا للحماية.

يتوقف اعتماد تقنية التعرف على بصمات الأصابع Fingerprint Identification Technology على طراز الكمبيوتر.

للحصول على مزيد من المعلومات، تفضل بزيارة الموقع: http://h18000.www1.hp.com/solutions/security.

الإعلام عن الخطأ والاستعادة Fault Notification and Recovery

تجمع ميزات الإعلام عن الخطأ والاستعادة (Fault Notification and Recovery) بين تقنيات الأجهزة وتقنيات البرامج المبتكرة لمنع فقدان البيانات الهامة ولتخفيض زمن التوقف غير المتوقع عن العمل.

عند حدوث خطأ، يعرض الكمبيوتر رسالة تنبيه محلي (Local Alert) تحتوي على وصف للخطأ والإجراءات الموصى باتخاذها. يمكنك عندها عرض الحالة الجارية للنظام باستخدام HP Client Manager. إذا كان الكمبيوتر موصولا بشبكة اتصال تتم إدارتها بواسطة HP Insight Manager، أو HP Client Manager أو تطبيقات أخرى لإدارة النظام، يرسل الكمبيوتر أيضا إعلاما بالخطأ إلى التطبيق المسؤول عن إدارة شبكة الاتصال.

نظام حماية محركات الأقراص Drive Protection System

نظام حماية محركات الأقراص (DPS) هو أداة تشخيص مضمنة في محركات الأقراص الثابتة الموجودة في أجهزة كمبيوتر HP مختارة. تم تصميم DPS للمساعدة في تشخيص المشاكل التي قد ينتج عنها استبدال غير خاضع للكفالة لمحرك قرص ثابت.

عند تصنيع أجهزة كمبيوتر HP، يتم اختبار كل محرك قرص ثابت تم تثبيته باستخدام DPS، وتتم كتابة سجل دائم يتضمن معلومات هامة في محرك القرص الثابت. في كل مرة يتم فيها تشغيل DPS، تتم كتابة نتائج الاختبار في محرك القرص الثابت. وباستطاعة موفر الخدمات استخدام هذه المعلومات لمساعدتك على تشخيص الحالات التي جعلتك تشغل برنامج DPS. للحصول على الإرشادات المتعلقة باستخدام DPS، راجع *دليل استكشاف الأخطاء وإصلاحها*.

وحدة تزويد بالطاقة تحتمل التغير المفاجئ في الفولتية

توفر وحدة التزويد بالطاقة التي تحتمل التغير المفاجئ في الفولتية ثقة أكبر عند تعرض الكمبيوتر لمثل هذا التغير. وقد تم تصنيف وحدة التزويد بالطاقة هذه بحيث تحتمل تغيرا مفاجئا في الفولتية قد يصل إلى ٢٠٠٠ فولت دون التسبب في توقف النظام عن العمل أو فقدان البيانات.

المتحسس الحراري

ميزة المتحسس الحراري هي عبارة عن أجهزة وبرامج تتعقب درجة الحرارة الداخلية للكمبيوتر. تعرض هذه الميزة رسالة تحذير عندما تتجاوز الحرارة النطاق المحدد، مما يعطيك الوقت الكافي لاتخاذ الإجراء المناسب قبل حدوث عطب في المكونات الداخلية أو فقدان البيانات.

الفهرس

A

ActiveUpdate، ٦
Altiris، ٤
Altiris PC Transplant Pro، ٥

C

cautions
protecting ROM، ٧
Computer Setup Utilities، ١٠
cover lock، smart، ٤٢

D

DiskOnKey
انظر أيضاً HP Drive Key.
قابل للتمهيد، ١٣
Drive Protection System، ٤٨
Drivelock، ٣٩؛ ٤١

F

FailSafe Boot Block ROM، ٨
FailSafe Key
طلبه، ٤٤

H

HP Client Manager، ٤
HP Drive Key
قابل للتمهيد، ١٣

P

Preboot Execution Environment (PXE)، ٣
Proactive Change Notification (PCN)، ٦
protecting ROM، caution، ٧
ProtectTools Embedded Security
Emergency Recovery Key، ٣٢
استرداد في حالات الطوارئ، ٣٥؛ ٣٩
كلمات مرور
Basic User، ٣٤
Emergency Recovery Token، ٣٢
Setup، ٣١
Take Ownership، ٣٢
ProtectTools، حماية مضمّنة، ٣٠؛ ٣٩
PXE (Preboot Execution Environment)، ٣

R

Remote ROM Flash، ٧
Remote System Installation، الوصول إليه، ٣
ROM
Remote Flash، ٧
ترقيتها، ٧
غير صالحة، ٨
ROM، أضواء لوحة المفاتيح، جدول، ٩

S

Smart Cover FailSafe Key، طلبه، ٤٤
Smart Cover Lock، ٤٤
إقفاله، ٤٣
إلغاء إقفاله، ٤٣

Smart Cover Sensor، ٤١
تعيينه، ٤٢
مستويات الحماية، ٤١
SSM (System Software Manager)، ٦
System Software Manager (SSM)، ٦

U

URL(مواقع ويب). *انظر* مواقع ويب.
USB flash media، جهاز قابل للتمهيد، ١٣

W

Web sites
ROM Flash، ٧

أ

أحرف محددة، جدول، ٢٩
أدوات الاستنساخ، برامج، ٢
أدوات النشر، برامج، ٢
أضواء لوحة المفاتيح، ROM، جدول، ٩
أنظمة التشغيل، معلومات هامة حولها، ٢٠
أولي، تكوين، ٢

إ

إدخال
كلمة مرور الإعداد، ٢٧
كلمة مرور بدء التشغيل، ٢٦
إعداد
أولي، ٢
تكراره بشكل متطابق، ١٠
إعداد عن بعد، ٣
إعداد، كلمة مروره
إدخالها، ٢٧
إعلام بالتغييرات، ٦
إعلام عن الخطأ، ٤٨
إقفال Smart Cover Lock، ٤٣
إلغاء إقفالSmart Cover Lock، ٤٣
إنذارات
حماية بواسطة قفل الغطاء، ٤٢

ا

استرداد البيانات المشقرة، ٣٥؛ ٣٩
استعادة النظام، ٨
استعادة برامج، ٢
الإعداد، كلمة مرور
تعيينها، ٢٥

ب

بدء التشغيل، كلمة مرور
إدخالها، ٢٦
برامج
Computer Setup Utilities، ١٠
FailSafe Boot Block ROM، ٨
Fault Notification and Recovery، ٤٨
Master Boot Record Security، ٤٥؛ ٤٦
Remote ROM Flash، ٧
Remote System Installation، ٣
System Software Manager، ٦
استعادتها، ٢
تحديثها على أجهزة عديدة، ٦
تعقب الموجودات، ٢١
دمجها، ٢

ت

تجزئة القرص، معلومات هامة، ٤٧
تحكم بالوصول إلى الكمبيوتر، ٢١
تخصيص برامج، ٢
ترقية ROM، ٧

تشخيص، أداة لمحركات الأقراص الثابتة، ٤٨
تعقب الموجودات، ٢١
تغيير أنظمة التشغيل، معلومات هامة، ٢٠
تغيير كلمة المرور، ٢٨
تغيّر مفاجئ في الفولتية، وحدة تزويد بالطاقة تحتمله، ٤٩
تغيير، إعلام به، ٦
تقنية التعرّف على بصمات الأصابع، ٤٨
تكوين زر التشغيل، ١٩
تهيئة القرص، معلومات هامة، ٤٧

ث

ثنائي الحالة، زر التشغيل، ١٩

ج

جهاز قابل للتمهيد
DiskOnKey، ١٣
HP Drive Key، ١٣
إنشاؤه، ١٢؛ ١٨
جهاز USB flash media، ١٣
قرص مرن، ١٢

ح

حالات الطوارئ، استرداد، ProtectTools، ٣٥؛ ٣٩
حجرة متعددة الأغراض، حمايتها، ٣٩؛ ٤١
حذف كلمة المرور، ٢٩
حرارة داخلية للكمبيوتر، ٤٩
حماية
DriveLock، ٣٩؛ ٤١
ProtectTools، ٣٠؛ ٣٩
Smart Cover Lock، ٤٤
Smart Cover Sensor، ٤١
إعدادات، إعدادها، ٢١
بواسطة كلمة مرور، ٢٥
حجرة متعددة الأغراض، ٣٩؛ ٤١
سجل التمهيد الرئيسي، ٤٥؛ ٤٦
ميزاتها، جدول، ٢٢
حماية محرك القرص الثابت، ٤٨
حماية مضمّنة، ProtectTools، ٣٠؛ ٣٩

د

داخلية، حرارة الكمبيوتر، ٤٩

ذ

ذاكرة ROM للنظام غير صالحة، ٨

ز

زر التشغيل
تكوينه، ١٩
ثنائي الحالة، ١٩

س

سجل التمهيد الرئيسي، حماية، ٤٥؛ ٤٦

ص

صورة برامج مثبتة مسبقاً، ٢

ط

طلب FailSafe Key، ٤٤

ع

عناوين إنترنت، *انظر* مواقع ويب.

ق

قرص قابل للتمهيد، معلومات هامة، ٤٧
قرص، استنساخه، ٢
قفل الغطاء، حماية، إنذار، ٤٢
قفل كبل، ٤٧

ك

كلمة مرور
ProtectTools، ٣١؛ ٣٤
الإعداد، ٢٥؛ ٢٧
بدء التشغيل، ٢٦
تغييرها، ٢٨
حذفها، ٢٩
حماية، ٢٥
مسحها، ٣٠
كلمة مرور الإعداد
ProtectTools، ٣١
تغييرها، ٢٨
حذفها، ٢٩
كلمة مرور بدء التشغيل
تغييرها، ٢٨
حذفها، ٢٩

ل

لوحة المفاتيح، أحرف محدِّدة، في المحلية، ٢٩

م

متحسس حراري، ٤٩
محرك أقراص، حمايته، ٤٨
محركات أقراص ثابتة، أداة تشخيص، ٤٨
محلية، أحرف محدِّدة في لوحة المفاتيح، ٢٩
مسح كلمة المرور، ٣٠
مواقع ويب
Active Update، ٦
Altiris، ٥
Altiris PC Transplant Pro، ٥
Fingerprint Identification Technology، ٤٨
HP Client Manager، ٤
HPQFlash، ٨
Proactive Change Notification، ٦
Remote Rom Flash، ٧
System Software Manager (SSM)، ٦
دعم البرامج، ٢٠
نسخ ROMPaq، ٧
نسخ متطابق للإعداد، ١٢
نشر PC، ٢

ن

نظام، استعادته، ٨

و

وحدة تزويد بالطاقة تحتمل التغيّر المفاجئ في الفولتية، ٤٩
وصول إلى الكمبيوتر، التحكم به، ٢١